Wrocław University of Science and Technology
Department of Quantum Technologies
Faculty of Fundamental Problems of Technology
CompSecur IT Solutions
The National Center for Research and Developement
Supported by the NCBiR project POIR.01.01.01-00-0173/15 Jurand

Quantum random number generators with entanglement for public randomness testing

Janusz E. Jacak[1], Witold A. Jacak[1], Wojciech A. Donderowicz[2], Piotr Jóźwiak[3], Lucjan Jacak[1]
[1] Dept. of Quantum Technologies, Wroclaw University of Sciecne and Technology, Wroclaw, Poland | [2] CompSecur Sp z o.o., Wroclaw, Poland | [3] Dept. of Applied Informatics, Wroclaw University of Sciecne and Technology, Wroclaw, Poland

THE PROTOCOL IN THE IDEAL CASE
(ideal measurements and ideal entanglement)

1. Preparation of the initial state in form of the uniform sum of such kets, that each of them has identical sum modulo 2 of every single qubit states defining that ket (described in the computational basis) – the XOR rule.
2. Individual local measurements of all qubits.
3. Repetition of the first two steps n times.
4. Obtaining n-bits long sequences, S_{Q_1}, S_{Q_2}, S_{Q_3}, ... corresponding to sequences of measurement results of qubits Q_1, Q_2, Q_3, ... accordingly.
5. Selecting a single sequence for public announcement in order to verify its randomness by a trusted third party (with arbitrary large computational resources).
6. After a successful randomness verification, selecting another sequence from those that are left, as a sequence which must never be used or published to ensure the secrecy of the remaining generated sequences, due to the XOR rule.
7. All the remaining sequences are truly random and can be used cryptographically.

THE PROTOCOL FEATURES

In the ideal case, due to the quantum entanglement all the sequences of measurement results, S_{Q_1}, S_{Q_2}, S_{Q_3}, ... share the same statistical properties – deviations of frequencies of occurrences in sets of patterns of the same length are identical for all of those sequences in the limit of sequences length n tending to infinity. In case of k entangled qubits Q_1, Q_2, Q_3, ..., Q_k ($k > 2$), a successful verification of randomness of only a single sequence S_{Q_i} proofs the randomness of all $k-1$ remaining sequences.

Randomness verification of sequence S_{Q_i} can be performed publicly, leaving the secrecy of remaining sequences ($k-1$) intact, provided that another single sequence (from the remaining sequences) S_{Q_j} ($j \neq i$) will be kept in secret and never be used – which leaves $k-2$ secret sequences with the randomness proven by the sequence S_{Q_i} randomness verification result and ready for cryptografic usage.

Public testing allows to perform an arbitrary complex testing (up to verification of deviation from statistical prediction of occurrences of all possible patterns for n-bit tested sequence, which is a very challenging task in terms of computational resources) overcoming the strong restrictions of computational resources nature of the local randomness testing possibilities of the QRNG controlling unit or of the QRNG itself. However, public testing should be performed by a trusted party, or as a service within a reputation based model, e.g. one with a blockchain type public testing results database, which will be discouraging to falsify tests results (reputation loss), and encouraging to test faster and more accurate (reputation gain).

Diminishing of an average time of the complex randomness testing (which in the case of e.g. finding patterns the execution times grows exponentially with the increase of the length of searched patterns) of finite length bit sequence. With the increase of the number of entangled qubits, the number of secret random bit sequences also increases. All of those sequences hold the same statistical properties (due to the nature of proposed protocol) – it is sufficient to test only a single sequence to get the information of the randomness of all other sequences. As the time needed to test a single sequence is fixed (it depends on the sequence length and does not change with the increase of entangled qubits), thus the average time (single sequence time divided by the number of sequences sharing the same statistical properties) can be brought to arbitrary small value.

THE PROTOCOL – 3-QUBIT CASE

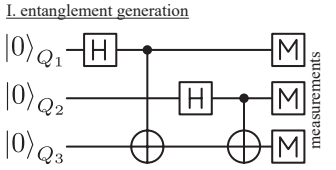
the simplest case of the proposed protocol:
3-qubit entangled state (with the XOR rule valued 0)

$$|\psi_{Q_1Q_2Q_3}\rangle = \frac{1}{2}\left(|000\rangle + |011\rangle + |101\rangle + |110\rangle\right)$$

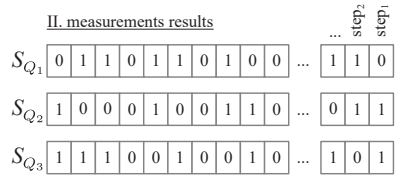
Alternative 3-qubit entangled state with the XOR rule valued 1

$$\frac{1}{2}\left(|111\rangle + |100\rangle + |010\rangle + |001\rangle\right)$$

I. entanglement generation



II. measurements results



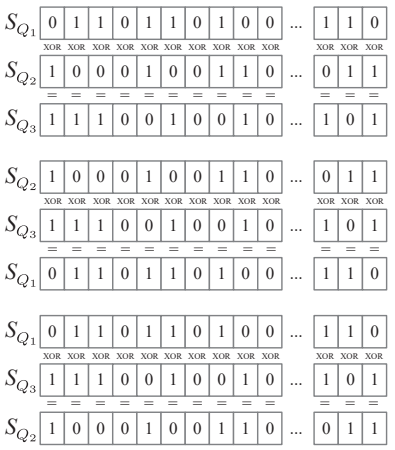
III. randomness testing and exemplary sequences usage

multiple trusted public testing authorities (for testing parallelization and mutual verification)

S_{Q_2}
– unpublishable
– unusable
– must be kept in secret to ensure secrecy of the usable sequences (a single sequence in the 3-qubit case)

S_{Q_3}
– free and secure for any cryptographic usage
– its secrecy is guaranteed, as long as S_{Q_2} is kept in secret
– its randomness is identical to the randomness of the tested S_{Q_1}

the XOR rule for 3-qubit case – each pair of bits in every step gives third bit when XOR-ed (this is the reason why one sequence must always be kept in secret)



A,*B*,*C*,*D* – possible correct measurement results; In the ideal case frequencies of their occurrences within S_{Q_1}, S_{Q_2}, S_{Q_3} should be equal for an arbitrary n

A	*B*	*C*	*D*
0	0	1	1
0	1	0	1
0	1	1	0

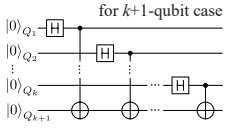
E	*F*	*G*	*H*
0	0	1	1
0	1	0	1
1	0	0	1

E,*F*,*G*,*H* – incorrect results indicating bias/error of source or measurement devices

THE PROTOCOL - GENERALIZATION

(k+1)-qubit entangled state – allowing to obtain k sequences with proven randomness (from which one must remain unused to ensure the secrecy of all the others sequences)

entanglement generator for k+1-qubit case



$$\left|\psi_{Q_1\ldots Q_{k+1}}\right\rangle = 2^{-\frac{k}{2}}\left(\prod_{i=1}^{k}\sum_{q_i=0}^{1}|q_i\rangle\right)|q_1 \oplus q_2 \oplus \cdots \oplus q_k\rangle$$

where for every element in the final sum in theirs last to the right ket (in above the ket with sums modulo 2), the q_1,...,q_k are valued by according values of the proceeding k kets of that sum element

MULTIQUBIT ENTANGLEMENT FOR RANDOMNESS TESTING

The protocol was initially proposed and described in 2017 in the patent application [1] and in 2020 was published in Sci. Rep. [2]. That publication coincided in time with announcement by the Google team of the quantum supremacy [3], which also was based on exploiting the multi-qubit entanglement to the problem of the randomness verification. We believe, that to some extent, both of those concepts are similar and even equivalent in the fundamental sense. In proposed protocol, in the ideal case, the randomness of the single sequence proves the randomness of all the other sequences, whose number corresponds with the number of entangled qubits. When those sequneces are concatenated into a one long sequence, then its lenght corresponds with the number of entangled qubits, but its randomness is still proven by the randomenss of a short single sequnce of the initial length. In other words, with the increase of the number of qubits composing multi-qubit entanglement the complexity of the randomness testing decreases, as with the same amount of the computational resources one can test much longer sequences. This interesting observation seems to shed a new light on how to understand fundamental concepts behind recently reported quantum supremacy for the randomness testing.

[1] J. A. Jacak, W. A. Jacak, W. A. Donderowicz, and L. Jacak. Entanglement quantum random number generator with public randomness certifcation. 2017. PCT/PL2017/000133-WO/2019/132679.
[2] J. A. Jacak, W. A. Jacak, W. A. Donderowicz, and L. Jacak. Quantum random number generators with entanglement for public randomness testin. Scientific Reports, 10:164, 2020. https://doi.org/10.1038/s41598-019-56706-2
[3] Frank Arute, Kunal Arya, Ryan Babbush, et al. Quantum supremacy using a programmable superconducting processor. Nature, 574:505, 2019. https://doi.org/10.1038/s41586-019-1666-5

THE PROTOCOL IN NOT IDEAL CASE

In not ideal case, when entangled states and/or measurements are not perfect, the statistical coupling between sequences S_{Q_1}, S_{Q_2}, S_{Q_3} will drop. This can be countered by entanglement purification procedures and the quantum error correction schemes – allowing to arbitrarily closely approach the ideal case at the cost of effectiveness drop, caused by increased redundancy for the control elements of the error correction schemes. Some methods to detect biases can also be proposed (it is enough to consider 3-qubit case without loss of generality).

Imperfect situation:
1. not properly entangled/biased initial state and ideal measurement devices,
2. perfectly entangled initial state and biased/erroneous measurement devices,
3. not properly entangled/biased initial state and biased/erroneous measurement devices.

Exemplary countermeasures to detect biases:

ad 1. Due to a possible bias, the initial state could be prepared in such a manner that the resultant sequences S_{Q_i} would not inherit identical statistical properties (e.g. for initial state in form $1/\sqrt{2}(|000> + |011>)$, S_{Q_1} will contain only 0s and S_{Q_2} and S_{Q_3} will be identical but with random distribution of 0s and 1s – clearly not all three sequences have the same statistical properties. Countermeasure here is a redistribution, in an uniform manner, of the bias among 3 sequences S_{Q_i}, by randomly selecting in each step of the protocol which Q_i measurement results will be appended to the S_{Q_1} (such selection requires two random bits at each step in 3-qubit case).

ad 2. In case of biased measurement devices the resultant sequences S_{Q_i} may also not inherit identical statistical properties. E.g., measurement device no.1 (measuring qubit Q_1) may be biased to always yield 0 independently of qubit Q_1 real state. This will produce a S_{Q_1} of only 0s and other sequences will definitely have different statistical properties. Thus similarly as in 1. it is important to redistribute uniformly and randomly those biases in all sequences S_{Q_i}, but here, by randomly selecting the measurement device which will perform the last measurement, which correct result is known from first two measurements, what allows to reveal the bias by the XOR rule (such selection requires two random bits at each step in 3-qubit case).

ad 3. The randomization of qubits numbers and measurements orders should be applied simultaneously and the results should be checked for errors violating the XOR rule (c.f. disallowed results *E*,*F*,*G*,*H* in the figure above). As those randomizations are internal and private, thus it is possible to use for this purpose generated in preceding generation cycle two sequences (the one published for testing, and any other unpublished, alternately concatenated, for both to be present in every two bits). The same two random bits can be used for both selections. This requires also the initial random sequences to be used in the first protocol run – resulting not in a quantum random number generation but rather a quantum randomness expansion, allowing to statistically detect the biases or errors, either as unnatural deviation of occurrence of patterns in tested sequence, or as a violation of the XOR rule. In the case of the XOR rule violations, it also possible to verify the character of those violations, by checking (similarly as in the randomness testing procedure) the occurrences of these violations along the entire sequence (with indicated bit positions within this sequence where violations occurred), and specifying whether those occurrences are truly random (nondeterministic errors) or not (deterministic biases).